THE

Final Straw

A WEEKLY ANARCHIST SHOW

The Final Straw is a weekly anarchist and anti-authoritarian radio show bringing you voices and ideas from struggle around the world.

You can send us letters at:
The Final Straw Radio
PO Box 6004
Asheville, NC 28816
USA

Email us at:
thefinalstrawradio@riseup.net
or **thefinalstrawradio@protonmail.com**

To hear our past shows for free, visit:
https://thefinalstrawradio.noblogs.org

To support transcription and zine-making efforts which are funded by donations, visit:
https://thefinalstrawradio.noblogs.org/donate/
or via Patreon:
https://www.patreon.com/tfsr
or via LiberaPay, which does not take a cut of the payments:
https://liberapay.com/The-Final-Straw-Radio/

Surveillance Self Defense, Encrypted Chat Apps and Securing Devices with Thorin Klosowski

Feb. 16, 2025

The Final Straw Radio

ty Project, where we wanted universities to set up Tor nodes because they just have the infrastructure to do so in a way that is much stronger than regular people can. And those exit nodes required a lot of legal stuff that is over my head that I'm not going to try to get into here because there is a different implication for a lot of that. But I think it's like anything, it's a tool that can be misconfigured or misused in a way that might lead to a false sense of security.

TFSR: I've kept you on for a long time, and I really appreciate you taking the time to have this chat. So there's ssd.eff.org, Surveillance Self-Defense. Are there any other resources? You've mentioned a few, like TechCrunch, Verge, 404 Media as resources where people could do some more research into digital security if this is an area that they're interested in. Any other things you want to shout out before we close up the chat?

Thorin: Yeah. I love Consumer Reports as a security planner. It is a great resource, especially if you're new to this. It is a welcoming resource that walks you through a lot of the core fundamental steps. So when we were talking about password managers and two-factor authentication, if that all felt very overwhelming, it's a great place to start your journey because the way the website works is it kind of does a little threat modeling for you. It asks you what you own and what you want to protect, whether that's like "I have an iPhone, I have a Windows computer, and I have a smart doorbell" or whatever, and then it builds a little plan for you to follow, and it just teaches you the fundamentals in a very welcoming way, and it's well done. It's available in English and Spanish.

SSD is available in a lot of languages, so especially if you speak a different language, or if you work with communities that are not English-speaking, we have a lot of resources in that way too.

TFSR: Yeah, that's great. I'm glad that you brought that up, because I didn't even think to ask. That's super helpful. Thorin, thanks for having this conversation and for the work that you do, and I'm excited to share this with the listeners.

Thorin: Cool, yeah, of course.

are just all of these different problems with VPNs that are on the fringes of different uses. There's been a couple of recent bugs around whether or not they're fully encrypting traffic. So using it as a security tool on a public network, is not really that useful, because it would be very easy to tap into that and access what they're doing. Corporate VPNs have had some recent stories about weird quirks there. It's just, kind of like everything else where it's very difficult to keep up with a lot of that, and I would recommend not really trying unless it's your field.

TFSR: Just to complicate this a little bit more, one concern that civil libertarians or other activists have had in the past about Tor is that people have complained about the funding sources for the initial program being a product of Naval Intelligence Research.

The way that it works is you connect to a network, and there are nodes that your data travels through that obscure the apparent path of your data, and that's what makes it hard to track where you're communicating from, I guess, and therefore where you're communicating to. Those nodes are physical infrastructure. Like hen people say the cloud is someone else's computer out there, nodes are on someone else's computer out there, and the NSA, over the years, has been running more and more of those nodes. People have been concerned that by having a large amount of that infrastructure in their hands, they would be able to get more information about A) who's using it and B) what they're using it for.

So this is a niche question, but if someone is concerned about the recent swing that a certain federal government has taken politically (and maybe they should have already been concerned about it), but how can that figure into their safety plan? Should it?

Thorin: Those nodes won't have access to the websites you're visiting or who you are because of the way they run through everything. But it is possible to know that you are using Tor, and it is possible to misconfigure Tor. So I think it's sort of similar to how we were talking about with Signal, where there's a couple of ways where things can go wrong, and that's something to consider.

Tor will not keep you anonymous if you're logging into your Gmail account or whatever. The way that all of those bridges work, the person running it won't see who you are, but that final exit node will know your traffic, but it won't know where it's coming from or who it's coming from, if that makes sense. When you're using Tor, your web browsing goes through a number of these nodes. The exit node is one of the most important ones and one of the ones that is a little bit more critical to run.

We ran a project, a couple of years ago, a year ago, called The Tor Universi-

This week, a conversation with Thorin Klosowski of the Electronic Frontier Foundation about some basic tools and ideas for keeping our information a little safer online and the Surveillance Self-Defense site, **ssd.eff.org** . We discuss device encryption, tor-browser, vpns, encrypted messaging apps like WhatsApp, Signal and Telegram as well as password vaults. I'm hoping this'll be the first of a few interviews to try to make digital security concepts a little more accessible.

Surveillance Self-Defense site: **ssd.eff.org**

Search for this interview title at **https://thefinalstrawradio.noblogs.org/** to find links to further resources on this topic, featured music, the audio version, and files for printing copies of this episode.

TFSR: Would you please introduce yourself with your name, pronouns, and affiliations?

Thorin Klosowski : My name is Thorin Klosowski. I'm a privacy and security activist at the Electronic Frontier Foundation. Pronouns are he/him.

TFSR: Thanks for being on this chat and all the work that you do. I wonder if you could talk a little bit about the Electronic Frontier Foundation (the EFF), what its aims are, and the work that you all do there. Its history is kind of cool, but we have a lot to cover here.

Thorin: The EFF is a nonprofit. It's been around for over 30 years at this point. Its main thing is that it fights for digital rights. What does that mean? It kind of has meant different things over the last 30 years. It's ranged from protecting the right to use encrypted chat tools to fighting against digital rights management to advocating for privacy laws.

We do this in three teams, basically. We have a legal team that works on everything from model bills on a state and federal level to impact litigation. We have a technology team consisting of technologists who study malware and research and consult on encryption techniques. They work on different tools like Privacy Badger, which is our browser extension that helps block trackers in your web browser. And then there's the activism team, which is the one that I'm on. We're the ones that help explain a lot of what everyone else does to the general public. So everyone works on different sections, and we all work together, and we're one of the few nonprofits in this space that operates this way.

TFSR: Using the terms digital security, information security, safety, and privacy, these terms are easily applicable to several different subjects. You all fall under what I would call a civil liberties perspective, which is focused on the individual and communities, as opposed to advocating specifically on behalf of corporations or government entities and invoking and protecting those rights. Can you talk a bit about how that shapes the way that you interface with courts, government institutions, corporations, and the framing that you operate from in that way?

Thorin: Yeah, I think the framing is trying to figure out how all of us can have a better time online, to simplify it down to its bare bones. I think that's the core principle. And that might mean pressuring corporations to maybe encrypt DMs [direct messages]. It might mean pressuring governments to pass a comprehensive privacy law. It might mean helping other organizations communicate securely and private-

TFSR: Maybe you're not so much concerned about obscuring, you're in a state where abortion has been made illegal, and you want to do research. Or pornography or whatever. A bunch of states in the southeast have blocked a bunch of porn sites. It's not the states that have blocked them, I guess the websites have blocked IP addresses that appear to be coming from places where the states have told them not to share this content. And I'm sure that's the same for political content or other political content. I guess that's a separate debate. So accessing something that maybe the provider is in agreement with the authorities where you live as to "You should not have access to this piece of information."

Thorin: Yeah. And that's kind of the one thing that VPNs are good for. They're good for shifting your web traffic to make it look like it's coming from somewhere else. VPNs are complicated because they have a long history of over-promising what they can do, and I think there's a misunderstanding of what they are capable of. But when it boils down to it, what they are good at is shifting your location. So if I am in California, I can pretend like I am in Sweden or in Texas, wherever.

The things to consider with VPNs are it might feel like that is protecting all of your traffic and information from your Internet service provider or even a government, perhaps, but all of your traffic is going through the VPN, so the VPN has access to everything that you're doing in the same way that an Internet service provider would. So it's not really a security tool or even a privacy tool. It's really just a way to shift your web traffic and where you are to appear like you're coming from somewhere else. I think that's the best way to think of it. Obviously, I would rather we had strong federal laws that were protecting even the need to do this, instead of having to download some weird tool. But thinking about VPNs, that's kind of the extent of what you will want to ever use it for or consider it about.

TFSR: And so as with trusting any platform that's being operated by an organization, there's the question of is this organization trustworthy if it can see some of the traffic or all the traffic that is passing through their network? There are a lot of different VPN providers out there. There are tons of people who rate them online for how safe they are, what sort of leaks there are of information. There's a free one that's available through Riseup that will give you a few different endpoints. But it's not foolproof, I'm sure. And I've heard that there could be leakage with IPv6, with the different location identification. I guess you could say information that's in that newer format. Is that correct?

Thorin: I don't know about that specifically. One of the other quirks is that there

and you type in google.com, it's going to run that through a few other computers to make it so it's very difficult to trace back to who you are when you're searching for it. The kind of beauty of Tor, to me, is similar to Signal where it just works out of the box. It doesn't really require a lot of finagling or setup. You can change settings if you have different concerns, or if you're in a country where you're running into very complex censorship, they have ways to help you get around that.

But for a lot of people, especially in the US, you just download the browser and you use it like any other browser, and that kind of just does it all automatically. A nice thing the Tor also does is it doesn't save your browsing history, which we've seen used as evidence against people often enough that it's something to think through. Your browser saves everything that you're doing. That's a lot easier to access than, say, subpoenaing Internet service provider. So yeah, that's Tor.

TFSR: Just on that too. I mean, a downside of Tor for a lot of people, might be that a website won't load because they're visiting it from a Tor browser. Is that correct?

Thorin: Yeah, it won't load, or it'll be slow. Because it blocks all trackers and all of the things that the Internet uses to figure out where you are and who you are, some stuff just won't work. Video is probably the biggest example of that. A lot of shopping sites don't work very well, but it's useful for researching information. I would say that that's like the best thing to use it for if you're just trying to learn about something mostly text-based. There are steps to take that even further in onion-based sites, which take that anonymization to another level, where, instead of going to the public-facing URL of eff.org, you would go to our onion site, which is hosted on Tor, and it is just even more private.

TFSR: Yeah, and Tor stands for The Onion Router, as in it's got these multiple layers, these skins that you have to go through to get to the core, which kind of obscures the path, right? So if people talk about onion sites, they're referencing that protocol.

Thorin: Yeah, It's been a part of my brain for so long that I kind of forget the foundational things.

TFSR: I was just imagining somebody trying to stuff a chop of onion into a USB drive, and I was like: "No, don't!"

Thorin: I mean, you know, maybe that is what we all need to do.

ly on their own. So we just tackle it based on what the needs are at that moment and focus on getting people the kind of privacy rights and just general rights that they deserve to have online, whether that's being able to speak freely or to control moderation on a social media platform, helping people get their voice out, helping people communicate safely and securely.

TFSR: Can you talk a bit about Surveillance Self-Defense [the website], who it's aimed at, and why y'all have produced it?

Thorin: SSD was created a little over 15 years ago. Its main purpose was to help protect people from government threats. And over the last 15 years that's shifted a lot depending on what's going on.

The first big expansion in it was for an international focus to provide security advice to protesters, journalists, and activists in other countries, helping people define what they needed to do based on where they were, instead of providing one-size-fits-all security advice. That's been a foundation for how SSD has worked since then: to teach people the tools that they need to protect themselves online based on what they want to do and how they want to do it, instead of telling people what to do. So the purpose is to give people a security mindset instead of just a list of tools to download and use. And that's not really changed since it was originally created.

The audience has shifted a little bit as surveillance has become a concern for not just people worried about government surveillance, but also corporate surveillance, which expands the readership out to basically everyone at that point, once you have both of those entities. And so where it stands now is that SSD is really built for helping everyone define what terms they want to engage the Internet on and how to secure themselves in a way that they can do that privately and without information getting into the hands of people that they don't want it to.

TFSR: I've had conversations with people in the past who have just said, "Well, I'm not doing anything wrong. Why should I care who gets what information off of me?" That elevator pitch. How do you interface with that argument?

Thorin: With the argument that we've all heard many times: "I'm not doing anything wrong. Why do I have to care?" There are two ways to engage with it, and it really depends on the type of person you're talking to. There are more than two ways, of course, but I tend to think of it in two different ways.

One is that you don't have anything to worry about right now, perhaps, but as we've seen, laws change, administrations change, threats change, and what was legal yesterday may not be legal tomorrow. The conversations that we have, the

products that we buy, the websites we visit, and the causes we donate to, all leave a history of who we are, and it's always possible that someone is going to come down on the opposing side of that, regardless of what your beliefs are. So that's one angle that is possible to take some people down.

Another one is frankly to call BS on anyone who says they have nothing to hide in that maybe you're not doing anything illegal, but the concept that you wouldn't be embarrassed or maybe a little shameful if parts of your life leaked out without your knowledge, whether that was your DMs at work or your purchase history off Amazon or your web history. You've probably said or done something that you don't want everyone to know about. And it seems unrealistic for me that no one has that feeling. I mean, maybe some people have no shame in them, but everyone deserves privacy because it's a right. It's a human right. And no one really should have access to our private conversations or our purchase history or any of that. It just seems fundamental to me that that is something that we can build on and have the conversation from there. If we don't agree on that, then it's a much more difficult argument to move forward, I think, with people, and I'm not sure you're gonna get very far in it.

TFSR: With the concept that I brought up of informed consent, I think it does say something, because most of us don't understand how the technology around us is developing, we don't necessarily understand what information is being collected, who it's being shared with, and under what circumstances.

If you're noting in your digital calendar the frequency of your menstruation cycle, and if that changes, is the app that you're putting this into, are they sharing the information, or is it accessible to law enforcement? If you live in a place where ending your pregnancy is suddenly off the books, it's no longer legal, what are the consequences of that? That may be a piece of information that you didn't realize that you were contributing to this ecosystem and that some company was harvesting. It may not be that you're doing anything illegal, you're just using this for your comfort.

I think there are a lot of unintended consequences, and I've heard people say over the years, I'm sure it's a bit trite and a bit oversimplified, but especially since there are so many free services out there and we're integrating this technology into so many parts of our life, that if there's not a price tag associated, if you're not paying for a product, then the information about you is the payment that you're making to the company. Does that still hold pretty true?

Thorin: I wish, but I don't think it does. Unfortunately, I think oftentimes, when

obscured from agencies, organizations, the person sitting next to you at the Cafe, whatever, that you're using the Internet on.

Can you talk a bit about some of the reasons that someone, for instance, in the US might want to obscure their web traffic and some easy tools that people can learn more about and start applying in their lives?

Thorin: I'm gonna start from actually the point of view that might be a little surprising to some people is that you're more secure than you probably might think you are on a public network because of HTTPS. This is so common now that you don't even see the lock icon in every browser, but for a long time, there was a little lock icon in the URL bar of a browser, and you would see that denoting that you were on a site that was taking security seriously.

Let's look at the network operator or the ISP, all they would see is that you went to a website. So if you went to eff.org, they would know you went to eff.org but they would not know you went to eff.org/thorinklosowski. I don't know why you would go to just my name, but... Yeah. So the amount of data that is easily accessible is less than people think.

For a very long time browsing the Internet on a public Wi-Fi network could be dangerous. If someone on that Wi-Fi network was monitoring all of the Internet traffic, and you were maybe shopping or banking, you're at the airport or coffee shop, and you're buying a T-shirt. 10 years ago, maybe you were on a website that did not have that little lock icon, and that meant that it could be possible for someone who was eavesdropping to maybe see a password as it traveled across the Wi-Fi network or a credit card number or whatever.

Nowadays, that's less of a thing. Most sites are encrypted with HTTPS, which means that from your computer to the server, it's encrypted. So if someone is on a Wi-Fi network looking at all the traffic, they wouldn't see anything, or the ISP wouldn't see the specifics of that information. So that's the good news there. But that doesn't mean that nothing is available. The websites you visit are still available.

In the US, there are some states that have criminalized certain things that other states have not, where you would be worried about what might be accessible to someone on the network. So if you are researching abortion in a state where it is banned or near-banned, that might be something that you would want to be concerned about. Or if you're looking at porn in a state where it is banned. I don't know if there is anything criminal there, but that is a reason why you might be looking for alternative ways to look on the Internet. There are two basic ways to do this: VPN or Tor are the simplest methods. There are ways to manipulate HTTPS traffic that can get you around things that we don't need to go into.

Tor is a web browser that works like any other web browser, except that it anonymizes your traffic through a series of different circuits. So if you open it up

messages on or an email address that you would be able to access from somewhere else. So that's the gist of it, and those two things combined can protect most of us from the simplest sorts of account hacks that can happen.

TFSR: I've had some friends that have worked at banks, for instance, and there's been an extra level of security where they've got a physical USB key that they have to have plugged in for an app to work or for the computer to even stay powered on or whatever, right? So it can get more complicated if your concerns are more complicated.

Thorin: Yeah, it can. So security keys are the gold standard for security, and as you said, it's a physical device. It's a USB key. They're usually shaped like keys, but not always. And that connects into your device, whatever it is, a phone or a computer, and usually it requires a tap or a touch before it'll authenticate. Those are good and strong because what they can do is protect against more sophisticated phishing attempts.

So not to get too technical, but if someone is just trying to get everyone, and they're just throwing out these phishing emails, you click on something, and you enter in your password, then it asks for an authentication, and that is done through an app of some kind. You physically type it in. There is the chance that that is all spoofed to get into an account. It's not super-duper likely, but it is possible.

A security key is more phishing-resistant in that it does more work to authenticate that you are where you are supposed to be. So if a website is www.goog1e.com, and you don't realize that it's not Google, it could trick you into entering all of that information manually, but a security key would protect that by knowing that you are not actually on google.com if that all makes sense.

TFSR: Yeah, absolutely. That's useful for sure. There is a ton of information that I would want to keep just popping questions at you. I want to reiterate, though, that for folks who are into reading introductions to some of the topics that we've been talking about, there are a lot of those on ssd.eff.org. Lots of step-by-step approaches towards concepts like encryption or your specific device or getting to know threat modeling concepts, which I think is super helpful.

People might not think about it in terms of us communicating information by visiting a website, but at a very foundational level, you're sending a request for information to this place that's sitting on someone else's computer out on the Internet, and it's sending information back. If we're considering that as important data, the searches that we do, the websites that we visit that might be a thing that we want to protect or keep

you are paying for it, you are still paying in data also. But you're getting at something that's fundamental in this problem, that we just don't know what happens to a lot of data.

Period tracking apps are a good place to start because there was a lot of worry around what data was going into those, and what was getting stored. In practice, a lot of what law enforcement was actually doing was accessing DMs or browser history or all of this other stuff that doesn't actually have to do with an app at all. So it's just when everything that we're doing is going everywhere, we don't know where to look, and we don't know what to focus on. We don't know how to tamp down on that. And because of the way the consent models work, there's no foundation for what privacy is, so for most of us, in most states, we just have to kind of feel it out. And it's not an excellent place to be. Let's say there's a period tracking app. You're looking in the app store, and there's a free one, and then there's one that's $2, and there's another one that's $4 a month. That doesn't necessarily automatically mean you're buying privacy at any of those tiers. Who knows anymore? And I think an interesting example of that would be something like streaming services, a completely different categories of apps, but they have ads, and those ads are often behavioral advertising based, which means that more than likely they are selling off whatever data they are collecting, and yet they also have a subscription model.

So that's a long way of answering the question: Does that hold true? Yes and no. I think in some tiers, in some categories of apps, it probably does. Maybe, if it's something that a small team of two or three people is working on, a notes app or something, they might have a more readable privacy policy, and maybe their business model is going to be clear in that you're paying $5 a month for the service and that is to pay their salary. Whereas a free one might be doing who knows what. So it can be used as a starting point, but it is not an ending point to that conversation anymore, I don't think.

TFSR: Rather than starting from a position of, "The universe is watching everything that I do right now," running and screaming down a hallway, can we talk a little bit about starting an approach towards security self-defense, or considering the way that we interact with the devices around us through threat assessment, threat modeling? Could you explain that approach? That'd be super helpful.

Thorin: Threat modeling is a scary set of words, so we tend to call it security planning because we've found that it tends to resonate with more people. It's the same thing. If you're familiar with threat modeling, security planning is the same. It just welcomes everyone in a little bit more. The concept is basically to ask yourself a series of questions to decide what kind of risks you might be willing to take with

the information or physical thing that could be gotten. So the questions that we like to frame this around are: What do I want to protect? Who do I want to protect it from? How bad are the consequences if I fail? How likely is it that I will need to protect it? How much trouble am I willing to go through to try to prevent potential consequences? And who are my allies?

If you ask yourself this series of questions about whether it's data you're trying to protect, or, you know... I'm in Los Angeles. There were recently wildfires just a few miles away from me. A question that I have to ask myself is: What goes in my fire-approved safe? What am I protecting it from? Fires. What are the consequences if I fail? It burns. How likely is it that I will need to protect it? Pretty likely, nowadays. And how much trouble am I willing to go through to prevent potential consequences? I'm willing to go through buying a fireproof safe and getting all of my documents that I need stored and putting them in there. And who are my allies? You know, neighbors, family. If I'm storing, say, some encryption code, I might store that with a family member on top of there in case something goes wrong.

That's just one example of running through that process and a very fast way on something that is kind of obvious. But the assets, what you want to protect can be anything, like your emails. It can be physical documents. It can be direct messages. It can be your location. If you're organizing a protest, it might be the collaborative documents you're working on with somebody. If you're a journalist, it might be your list of sources or your notes. If you're just a person in the world, you might not love corporations spying on every purchase you're making, so you want to stop trackers and try to prevent all of that as much as you can because you just don't like the idea of companies profiting off of you. And the same would go for AI models or social media companies, any of that. So it's the general concept of it. And I think for us, it's about handing people the tools to figure this stuff out on their own. And this is what we have found as one of the better ways to start people off.

TFSR: I think that that approach is super helpful, especially with news of malware like Pegasus. People could absolutely just go through the roof, and if they want to make that choice, that they don't want to engage in digital communication, that's totally reasonable, I think. But the idea that those technologies are going to be used against someone unless what they're holding is considered a high price target, like the amount of work, the amount of energy, and the monetary cost of applying those kinds of technologies to people. The "How likely is this to happen to me?" is it a very important part of that safety planning.

Thorin: Exactly. There are certain people who a malware company is going to be

at some random store where I am buying lumber. And five years in the future, that lumber company will suffer a data breach, and everyone who purchased anything off of there will be in this giant spreadsheet that includes their phone number and their name and their email and the password they used, and maybe their credit card. Then someone will come along and they will plug all that into a program, and they'll just start trying that username and password everywhere. Eventually, it's possible that they will land on my Gmail account or my Facebook account, and then they're into the whole thing. So they could kind of get into all of my accounts from there. The best way to help prevent that from happening is to use a unique password on every website.

The amount of accounts we all have is such an absurd number that it's basically impossible for most people to keep individual passwords in their head for everywhere. So there are programs called password managers that do this for you. Some of them are free. There's a chance that you've interacted with it on your iPhone or Android device, maybe without even fully realizing it, or your Mac or Windows device. What they do is they store the username. They usually generate a password. It's usually a long password that meets the password requirements on whatever page you're on. So it's got a character, and it's eight characters long, it's got a weird number sign and some numbers and everything. That way you don't have to remember it.

If you're using Apple or Android, it'll usually get locked behind your Google or Apple account. If you're using a third-party password manager, something like 1Password or Bitwarden, or a couple of popular ones, it'll all get stored inside of that, and that is locked behind one single password. That one single password should be very strong, unique. That's the one thing you do have to remember. The onus is still on you a little bit to need to remember something. It's that one password. So that's the one you'll want to make nice, strong, and long, not Thorin1234. So that's part one there.

Part two is to use two-factor authentication whenever it's offered and whenever it's possible. That is, if you've ever tried to log into an account and you'll get a text message with six numbers you have to type in before you can log in fully, that's two-factor authentication. The strongest way to do that is usually through a separate app that generates those numbers for you. But you might also find it in email or text messages. It appears in a variety of different ways. With Google, sometimes you'll log into an Android device, and it'll be like, "Confirm that this is you on YouTube from your computer." It all operates similarly but is kind of deployed differently.

The idea there is that even if someone does get your password, they cannot get into your account unless they have that second factor. That second factor is usually a physical, separate device of some kind, a phone that you can receive text

ing across borders, because my understanding is TSA or border patrol will enact national security claims in some instances and take people's devices. And in any case, you're separated from it, while you're passing through security zones.

Thorin: It's also useful to think about who you are and why you're traveling. I think if you're a journalist who's traveling for a story, and you don't have a phone, or you don't have something, that's going to cause as many alarms as if they found something. So I think you got to go through a lot of different questions here, which, again, is kind of why threat modeling and security planning are really useful for something like this specific instance. Because if you're just cruising around on vacation, there's a different set of concerns to have than if you're on a reporting trip or whatever else it might be.

TFSR: Maybe. [laughs]

Thorin: Fair enough, yeah.

TFSR: Concerning the topic of keeping a device secure or keeping your accounts secure, there's a lovely website out there called Have I Been Pwned that basically tracks when there is a known security breach and people's sign-in credentials for websites get leaked out. If they can get access to it, they will make mention. Can you talk a bit about passwords? How do we keep our devices and our information more secure through two-factor authentication and password vaults?

Thorin: Yeah. So I know I started this conversation by saying everyone's needs are different and you need to go through this whole process. But also, there is a core set of security advice that is pretty applicable to nearly everyone, which is: don't reuse passwords. And the easiest way to do that is to use a password manager. So you mentioned Have I Been Pwned, which is a site where you can type in your email address, and it'll show everywhere that your email address has appeared in a data breach that they were able to look at. So almost everyone is going to have at least one of their email addresses in there I would say at this point. The likelihood of your email never being included in a data breach is very close to zero, I would imagine. Unless you only have like three online accounts.

And something that a lot of people do is they'll reuse passwords across accounts. So if I have a Gmail account, I will make my password, and it's going to be Thorin12345, and then I will go over and I'll make a Facebook account, and it's going to be the same password, Thorin12345, and then I'll do the same thing

willing to burn a zero-day on, and there are a lot of people who are not. I think it is important to know if you are one of those people. If you are under an oppressive government, and you are a journalist there, or an activist, that is a very different position to be in than someone protesting here in the US even, which has its own set of risks, but it's different. And going through this process helps sort of tamp down on those fears a little bit. You can't protect everything all of the time. That's just not conceptually possible. So knowing where to focus your mind and your attention, at least for me, is something that calms me down a little bit. Obviously, not everyone's going to react that way, but it helps me.

TFSR: Or your proximity to someone who might be considered a threat. I mean, this is again, another rabbit hole. Like the journalist's Khashoggi wife, it turned out, had Pegasus or a similar app on one of their devices. Proximity to people who are considered to hold assets by powerful players can also make you a target.

So even with the US government, who a lot of the listeners to this would consider to be not on our side, not having our interests in mind. The FBI, for instance, considering their history of messing with social movements and individuals who are threatening the status quo, has said people should be shifting towards end-to-end encryption in their communication with each other, the way they do commerce, personal contacts, everything.

So I wonder if you could talk a little bit about the basic ways that we've communicated over the last couple of generations, or the last generation, and the way that computing and monitoring have changed how safe those methods are. And we can go from there about encryption itself.

Thorin: So if you take a step back and think through maybe your last week of your life and all of the ways you've communicated with people. You've probably communicated in person with somebody, maybe you've gotten a letter from somebody, maybe you've talked on the phone. Maybe you've text messaged somebody, maybe you've had some DMs on a social media platform, maybe you've had some DMs on something like Discord or Slack. Maybe you've talked on Signal or WhatsApp or Facebook. Maybe you've emailed somebody. We are all talking constantly to many people in many different ways across many different platforms. And many of those platforms have varying degrees of insight into what you are saying and doing.

So a phone call or a text message, an SMS message, could be monitored, whether that's by law enforcement with a warrant and intentionally, or if it's by the hackers who have gotten into US infrastructure. Something like Slack or Discord can be monitored by the company, whether it's a work-issued communication platform or school-issued, it could be monitored by the organization who's running

that. And then we have other tools at our disposal, like Signal, WhatsApp, and iMessage that are encrypted in a way that the platforms that run them can't see the contents of the communication. So that's kind of the playing field that we're in right now. The very short summary of it anyway.

TFSR: Around protests or investigations, or around prisons, if people are getting a hold of phones on the inside, law enforcement sets up devices that are sometimes called IMSI-catchers or StingRays. I'm imagining that they would need a warrant to do this, but I don't know. They would probably have to, because they'd have to be interacting with the FCC [Federal Communications Commission] about it. Law enforcement will use those devices to pretend to be a cell tower, and catch data in transit for use in an investigation or later use. If you send an email without using an encryption scheme, is that visible to people? And who is that visible to? Is that just visible to the people who run the two email services, the receiver, and the sender?

Thorin: Just to step one step backwards, with a StingRay, you would get text messages and phone calls. We don't have a ton of evidence about those being used at protests. We've been looking but nothing has popped up yet, but they are used for a variety of different reasons across the US, in more targeted ways, instead of just capturing everything in a location anyway, again from what we've seen. But for email, it would be visible to the platform holder and subject to a law enforcement request, because they would be able to access it. So the same way if you are sending DMs on X, those would have the same lack of protections. Or Instagram, for that matter.

TFSR: Maybe communicating, DMing sensitive information to someone else on X is not the best idea. But if we are concerned about either the corporations that run the platforms that we use currently or potentially in the future or the government that might be listening in, how do we harden our communication with other people? What are some good, accessible methods? You've mentioned WhatsApp and Signal, for instance.

Thorin: Yeah, so I think that framing is really nice because it encompasses now and in the future, which we've seen time and time again platforms shift ownership or direction or administration's change. Suddenly you might worry about your DMs on a platform that you were not worried about before. This, to kind of do a side hatch conversation, is a good example of why we could use strong encryption everywhere. I think in general, when people see direct or private message, they assume that it is a private message and not accessible by anyone. So they often assume they might have these sorts of protections when they don't. That's a different part of this

Thorin: It seems like it should stop it at all levels, although the way that this works, it's kind of difficult to say anything with a ton of certainty.

TFSR: Neither of us, as far as I know, are lawyers. I don't think I'm a lawyer, but can you talk about how... People travel with devices all the time. These devices have a ton of our personal communications. They may have sexy pictures. They may have your favorite games on them. You know, whatever. There's a ton of information. People put payment platforms and payment methods on their phones.

In terms of a US audience, who's the majority of listeners and who might be hearing this on the radio, can you talk about other places than in arrest where there appears to be, in practice, a liminality to your rights and your protections around devices and privacy? For instance, I'm thinking about when you're traveling either internationally or if you're at an airport. Is there a notable practice that's notable or different in your ability to keep a hold of your devices and potentially be pressured to open your devices for authorities? Could you talk about that a little bit?

Thorin: Yeah, as you said, neither of us are lawyers, so I don't know if I can answer this too narrowly. But I think a different question that might be useful to ask yourself if this is something you're concerned about is more: "If I go to another country or I'm at a border crossing, am I going to be willing to stand up to the person asking me to unlock that device?" And if the answer is that maybe not or no, then I think you can start going down a different path in deciding what you would want to do in that situation.

I know, from my point of view, if I am in Europe somewhere, I'm not going to know how to communicate that clearly or to say no. I'm just going to want to get home or whatever the case might be. So I don't know that I would trust myself to protect my phone or whatever in that circumstance. And I think if you're kind of in that same point of view, then I would reconsider what you might want to have with you at any given point because I certainly don't know the laws of every country or what access Poland's equivalent of the TSA is going to be able to do on my phone, you know?

TFSR: I know that when I fly internationally, I carry a different phone. Luckily, also in the United States, you don't have to register to get a SIM card. So if I am concerned about traveling across borders with a device that has the accumulation of information that comes with me in so many places, day-to-day, that I'm communicating with people on all sorts of different apps through, if my concern is to not have that accessible when I'm travel-

law enforcement agencies had access to Cellebrite devices where they could maybe not log into but could copy the information off of people's phones that were taken for, I guess later, slicing and dicing or attempting to break the encryption. Is that right?

Thorin: Yeah.

TFSR: So I guess that's an extra reason if you're concerned about laws changing, if you're concerned about the possibility of being punished in the future for something or being accused of something that you could face heavy charges for, I would say that not putting yourself in a situation where you have your phone on you if you think you might get arrested is like the best option.

Thorin: For most people that's kind of the better approach. Cellebrite is interesting—this isn't really security advice, just kind of a fun fact—because it tends to be about an update or two behind. We've seen some charts. I think 404 Media was able to get a hold of one of the more recent ones. They tend to be one or two update steps behind on iPhone and certain Android devices. Because of the way Android is developed. It's kind of up in the air. It's much more difficult to track there since every phone can use a different fork of Android. But it's a strong reason to make sure whenever you get that update warning on your phone to run the software update and let it go. It's kind of funny. My computer just popped up with one in the middle of this call.

TFSR: It's listening to us! [laughs]

Thorin: But a lot of a lot of those tools work off of bugs, basically. And those keep getting patched with every update. So it's kind of like a cat-and-mouse game. And one of the best ways to protect [yourself] is just always to keep your phone updated. It's not perfect by any means, but if you're in that middle ground where maybe you're like, "I don't know if I should be bringing my phone to this, but I would like to document it. I want to meet with my friends and don't want to get lost," whatever, the thing you can do is make sure your phone is updated, and that's going to be a big help in case you do get arrested.

TFSR: So that one or two levels behind on the updates or whatever on the Cellebrite, would stop them from getting access enough to be able to copy the information, even in an encrypted form, off of the phone, or is it about being able to break into that encryption?

conversation that I won't dwell too long on.

But apps like Signal and WhatsApp use end-to-end encryption, which means... The easiest way to understand it is that you and the other person in the conversation are the only people who can access the messages in it. So if you're using Signal or WhatsApp, that means that Signal as an entity or Meta/WhatsApp cannot see the contents of the messages you are sending back and forth. Or if you're on a phone call, they cannot listen in on what you're saying.

What it doesn't mean is that whatever happens once it gets to those two ends is invisible to everyone. So if you leave your phone unlocked and someone looks at your messages, obviously they can still see that. People can still screenshot things. All of those sorts of threats still exist. But the actual platforms running the companies won't see the contents of those messages. And that just gives you a private place to have a conversation with friends or to organize or whatever you need to do without needing to worry about the contents of those messages getting into a company or government's hands easily.

TFSR: So Signal is a company that was founded by anarchists and people who were known in hacker and developer communities. It has changed hands. It's no longer those specific individuals running it, but as a platform, it does have, it seems, a lot of oversight from within digital security worlds, people looking at the code, people noting bugs and fixing those bugs pretty frequently on the different platforms. It seems like a pretty robust community around it.

It's also an app that has not only been promoted internally among certain US government agencies for usage but also has been the bane of their research when they've been trying to get in and get messages from within it. So that, for me, not being a software developer and not being able to read code, those sort of trust models of who uses it, who swears by, what sort of accountability they have for these things, that's how I gauge my level of trust with a program or a platform.

Another couple of really commonly used apps that have the possibility of an end-to-end encryption are WhatsApp, which you've mentioned, which is owned by Meta and which a lot of people have concerns about trusting the platform, as well as Telegram, which a lot of the right-wing loves to use, apparently, and they don't look at the history of that corporation handing over personal data to whatever governments happen to want to repress people that are doing chats on Telegram. But I wonder if you could talk a little bit about how we assess platforms for their safety? How do we threat model against the platforms themselves?

Thorin: Yeah, I think we can take each of those in turn. So starting with Signal, as you said, it's robust. It's popular. A lot of people use it. There are a lot of people much smarter than I am, looking at the code, ensuring that it's doing what it says it's doing. It has been subpoenaed and not been able to provide anything. It's gone through a lot of different processes and we have a pretty good idea that it is operating as it's supposed to be.

WhatsApp uses the Signal protocol which is the end-to-end encryption design that Signal developed. We know that at least the core parts of WhatsApp are operating in a secure manner. It's so popular that a lot of people pay attention to what's happening on WhatsApp. There are concerns with what Meta collects in its metadata—wow, that's a hard sentence to say—because they are getting maybe time stamps or who is messaging who. They're not seeing the contents of the message, but they can see a lot around the message that can maybe give them some details about who you are and what you're communicating with. We haven't seen a lot of examples of how that might be used against somebody, but it is something that's definitely a risk. It's also one of the most popular platforms in the world.

T go back to threat modeling and security planning, if you're communicating with your grandparents in another country, WhatsApp is more than likely what you're using, and it's completely fine for most people to be doing so on there, and the contents of those messages should be remaining safe and secure.

Actually, let's go to Facebook Messenger, which you didn't mention, but should be included in this conversation because of its popularity. In Facebook Messenger, one-to-one conversations are also end-to-end encrypted, which is great and how that should be operating. But one-to-many conversations are not. So if you're in a group chat that is not end-to-end encrypted, which muddies the waters a little bit in kind of understanding what the security is, which I don't love, They've been saying they're working on group messages for a long time, and I hope they get there soon because it's confusing for people. Okay, so if I'm talking to one person, it's safe and encrypted, but if I'm talking to many people, it's not. It's just an odd way to do it, and it's hard for people to wrap their heads around. And that comes with the same kind of worries that you would have with Meta as an overarching company in general, the same as WhatsApp.

TFSR: Just on the note of that too, I know that when I've installed and uninstalled WhatsApp, WhatsApp wants access to my contacts saved in my phone, as opposed to when I have installed or uninstalled and reinstalled Signal or done the computer platform for it, it doesn't require that access. And it's pretty creepy. It doesn't need to have my contacts to do end-to-end encrypting. It just needs a number for one end and a number for the other, right?

Thorin: The good news there, in a roundabout way, is that device encryption is pretty common nowadays. Most devices that are purchased and set up within the last three or four years, probably have device encryption enabled practically by default, or at least they push you toward it. Unless you intentionally do not set a password, you are probably already using device encryption. So that's kind of good news. As long as whenever you set up your Windows computer, Mac computer, iPhone, or Android device, and you have a passcode or password, device encryption is more than likely on.

Let's even step back and broaden this a little bit to something that I think everyone can be concerned about, which is that if you lose your phone or it's stolen, the person who got it more than likely cannot get into it. Unless they can guess your password or passcode, or you are a very important person they have a very good reason to get into that [device]. But for most of us, if you just lose your phone, or it falls out of your pocket on the subway or whatever, the person who picks it up is not going to get into it, as long as you have a password on there.

And it does start to get a little bit in the weeds when it comes to using a biometric login, whether that's face or thumbprint, and those protections are good and strong for most people, most of the time, especially if they're just at home or whatever. But there's kind of shifting... [It's] unsettled legally on whether or not law enforcement can compel you to unlock a device using a biometric compared to a password. This starts to get into legal territory that I'm not going to try to pretend I'd fully comprehend, but it's unsettled, I guess, is the kind of shortest way to get to the answer.

So if you're in a situation where you feel like you may be compelled by law enforcement to unlock a device, it's usually best to turn off the biometric, whether that's face unlock or thumbprint. If you're going for example to a protest where maybe you'll get arrested, that's a good time to turn that off, even just temporarily. You can turn it back on whenever you're back home or back to your more day-to-day life where you're not concerned about that.

So this is a kind of short version of what's going on with device encryption. The good news is it's easy. It's everywhere. The bad news is it is possible to accidentally not turn it on. So if you don't unlock your device with a password, I would recommend going in and figuring out how to do that for whatever you're using, whether that's Windows or Mac or Android or iPhone.

TFSR: I remember a few years ago talking to a digital security professional about phones that were taken during protests. When people are arrested, oftentimes, their devices, their wallets, articles of clothing, and so forth, get separated from the individual when they're put into a cell and when they're being processed through. At least four years ago an incredible number of

on what that data processing is.

The point I'm trying to get at here is that every year there is some new hole in a lot of this that we have to think through, whether that's as a community of people using a service or as the providers. And there will be conversations around this all of the time, forever, and the best resources are probably tech journalists to look to figure out if something is legit or problematic or if something you need to be concerned about or a setting you need to change. I think sites like TechCrunch, 404 Media, even The Verge, if something gets this big, it's going to be reported on there, and you'll probably find a pretty good write-up on what's going on.

But it's one of the reasons why, personally, I find the default settings that an app launches with or a new feature launches with to be really important. It's about opt-in consent from a user's point of view, asking if I want an AI to summarize these messages or not, instead of just turning it on and doing it. I think it's a way that we engage with technology and something that we've been take advantage of for so long with a lot of this that it's very frustrating when it happens because it feels like this could have been easily avoided if you just asked your users what you want to happen. And unfortunately, it just does not happen very often anymore.

TFSR: To point back to the project that you work on, ssd.eff.org, I know that it has guides to different apps for encryption that one might approach and sort of introductions on how to set them up, right?

Thorin: Yeah.

TFSR: Cool. If folks are finding that we're a little bit in the weeds, and you want to get more detail with words in front of you that are easy to access, this is a good place to start.

There's data in transit. There's the communication between devices, and that's sort of what we've been talking about in terms of encryption. Some data is more static in terms of encryption, which I think is also important to talk about. As we mentioned, one of the biggest threats to the messages in your phone is when it first gets created on your device. What's the phone doing with that? Or the messages that are sitting on your computer that you may have locked with a thumb lock, your fingerprint, or whatever.

Can you talk a bit about device encryption approaches? I know there are a lot of different devices out there, and there are different locking methods, but what are some good resources, and what are some good approaches towards thinking about "Do I encrypt my hard drive on my computer," for instance?

Thorin: Yeah. I mean, neither of them needs it. WhatsApp just phrases it in a way that makes it sound like it won't work. But WhatsApp is completely fine without access to your contacts. Signal offers that and then it links you up with people that already have Signal accounts. So it's possible, but they just kind of phrase it a little bit differently in the onboarding, but both of them can operate without it totally fine.

TFSR: Cool, thanks. I just wanted to kick that in there, because that really annoys me about WhatsApp.

Thorin: Especially with the way that, at least on an iPhone now, you can select only certain contacts that would be given access or given over to the app, but then you have to sit there and plug each one in and tap in. It takes forever. It's a good step forward, but it's also kind of a design mess.

TFSR: Yeah, whereas on Signal, not only do you not have to share your contacts, but you can actually obscure people's ability to search for your signal identity by making your phone number no longer searchable on Signal, which I think is pretty cool.

Thorin: Yeah, and you can make a username now, so you don't even have to share your phone number to begin with. But to its credit a lot of this is because Signal was making choices as it went along. I remember whenever I first signed up for Signal, it alerted everyone that I just signed up for Signal. So it was a learning experience for them too.

TFSR: Do you want to talk about Telegram now that I've interrupted you?

Thorin: Yeah, so Telegram is kind of a weird example because it almost feels like... I can't even think of any really good examples of what it is. I guess Facebook would be the weirdest, closest analog because Telegram is not end-to-end encrypted by default, so you can have one-to-one messages, but you have to opt into that, which is how Facebook Messenger worked up until about a year, year and a half ago. You had to turn it on, which is something that if you don't know, you won't do. And it often gets misreported in the media that Telegram is an end-to-end encrypted app, which I guess it technically is. It offers that option, but I don't think that's usually what people think of when they think of it.

The beauty of Signal, and as you pointed out to a lesser extent WhatsApp, is that they just work, and you don't have to do anything special. You kind of just install it and you start using it, and you start communicating on it, and it works

just like you're used to, like iMessage with your messages which are also end-to-end encrypted, as long as everyone's got an iPhone. It just works like a chat app, and you don't think twice about that you're doing some hacker-crazy thing. You're just talking with your friend. And you can thumbs up, you can have emoji, you can do all the stuff. It's fun in that way, even if you're plotting a labor strike or whatever.

TFSR: Yeah. It's not like Element, for instance, which I hear is quite solid, but it also doesn't really communicate across platforms very well, and sometimes it gets reset, but at least you can self-host that.

Thorin: A lot of this is just getting people to use the thing. And way you do that is you make it fun to use or interesting to use or easy to use. That's kind of half the battle with a lot of this.

TFSR: So that's one criticism that's come up, and I've talked to folks a couple of times who were working on projects like Enigmail, attempting to create an easier approach towards using PGP for encryption for emails. Because email is great. You can host it. Tons of people that host it. You can apply the end-to-end encryption on top of it. It's less clunky now than it used to be, but it's still pretty clunky, and I'm not sure what kind of leakage there is for data of people using PGP.

Thorin: I mean, it's clunky and it's hard to use. It's prone to error. And I think the prone to error is the biggest problem. If you think you are communicating securely when you are not, that is a huge gaping hole to have in whatever you're doing. And for me that's a bigger risk. I would rather just stick to chat apps because they're significantly easier to use. Email if you know what you're doing, is totally fine, but the chances of everyone on that email chain knowing what they're doing is diminishingly low, I think.

TFSR: So we've agreed that Signal seems like a pretty trustworthy platform. More and more people are using it. Even governments use it for internal communication with their employees. One thing that comes up every few months on Signal chats that I'm in is someone sends a message that says, "Signal has been compromised! There's a new zero-day hack out there." These sorts of announcements flow through, and I see people make the same explanations, for the most part, every time: "This was a known thing on the specific phone platform that they patched. The manufacturers fixed it two years ago. It didn't affect this program in this way or you can turn off the setting and then that danger wouldn't be."

Like the location data, if you're not relaying phone calls and Signal which you have to go set up. Or someone's encrypted communication got accessed because they had a thumb lock or a face ID lock, biometrics of some sort to lock their phone, and law enforcement was able to put the phone in front of the person's face and get into the messages. Can you talk a bit about when somebody hears this message go through that Signal is compromised, how should they approach that news? Where can they go to find more information about it and better ways to handle that than just just passing it on?

Thorin: Yeah, I think to look at that cautiously, as we kind of talked about before. Signal specifically is looked at by a lot of people often, and the protocol is also used for WhatsApp, so expand that out and there are a lot of eyes on Signal all of the time. That does not mean that problems don't arise, bugs don't happen, people don't have their phones set up in a way that fits in their security model. All that Signal can do is control that it gets from point A to point B securely. What happens at the beginning of that stage and at the end of that stage is out of Signal's hands. So if, as you mentioned, law enforcement got access to a phone and they were able to unlock it and you didn't have disappearing messages on, they would see the whole chat history, just like they would with any other app they opened up. They would have access to everything.

Little bugs happen now and then with just general user settings. A few years ago, with the way registration worked, Twilio got hacked, and that was a phone platform that provided numbers that people were able to reset because there's an optional setting to turn on a pin that would require that pin if Signal was registered on a new phone. Kind of like how SIM swapping protection works with most cell carriers now. So there was not necessarily a problem with the Signal protocol or the Signal apps. It was a problem with a third-party service getting hacked that was then used to register Signal on new devices.

I haven't turned on a new Signal account in a while. I don't know if registration lock is required now, but that's one setting that I'd like to point people towards pretty early on to turn on, similarly to SIM swapping, because it's a good habit to get into to protect that.

And then the latest thing that I've seen is around AI and notifications, which is a thorny and weird problem that I think we're still kind of unpacking and figuring out what is going on. Apple does its AI summaries, which takes the collection of your most recent messages, and turns it into a shortened version of that, arguably in funny ways, sometimes in incorrect ways, but whenever that's happening Apple says it's on the device. I don't know that anyone's looked at it super closely. On Android, Gemini is used to do similar stuff, and it is less clear than Apple is